



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,503	09/02/2003	Len L. Mizrah	AIDT 1005-1	3753
22470 7590 08/23/2007 HAYNES BEFFEL & WOLFELD LLP P O BOX 366 HALF MOON BAY, CA 94019			EXAMINER HOMAYOUNMEHR, FARID	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 08/23/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/653,503	<b>Applicant(s)</b> MIZRAH, LEN L.	
	<b>Examiner</b> Farid Homayounmehr	<b>Art Unit</b> 2132	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 08 June 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-4, 6-11, 13-18 and 20-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6-11, 13-18, and 20-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This action is responsive to communications: application, filed 9/30/2003; amendment filed 6/8/2007.

2. Claims 1-30 have been considered. Claims 5, 12 and 19 cancelled by the applicant. Claims 22-30 are new.

### ***Response to Arguments***

3. Applicant's arguments in view of amendments have been found persuasive. The rejection under section 112 to claims 1-21 and rejection under section 102(b) is hereby withdrawn. See the new grounds of rejection in the next section.

### ***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 23, 24, 26, 27, 29, 30 rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are: the hash of the intermediate data key (n). The hash of the intermediate data key (n) is sent from

Art Unit: 2132

second station to the first station. However, the first station does not have the hash of the intermediate data key (n) to verify the item sent from the second station. This creates a gap between the elements involved in the process of key distribution.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-4, 6-11, 13-18, and 20-30 rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman, (US patent 6363480, March 26, 2002), and further in view of Kelly (US Patent No. 5,636,280, dated June 3, 1997).

7.1. In reference to claim 1:

Perlman discloses a method for producing ephemeral, symmetric encryption keys at a first station for mutual authentication and secure distribution of random session specific symmetric encryption key in a communication session with a second station, comprising:

- Assigning a session key in the first station, in response to a request to initiate a communication session received by the first station during a session key initiation

interval for use in a first exchange of a plurality of exchanges executed for distributing the symmetric encryption key produced for use in the communication session (the SSL protocol as exemplified in Perlman col. 2 lines 20-35, establishes a session key between the parties of communication);

- Associating, in the first station, a set of intermediate data keys, different from said session key, with said request for use in said plurality of exchanges (Perlman column 5, lines 55-67, where the ephemeral key pairs are announced as a list including other intermediary ephemeral key pairs)
- In the first exchange, sending at least one message carrying said session key to the second station (as mentioned above, SSL sets up a session key between the two parties), and receiving a response from the second station including a shared parameter, which is shared between the first station and the second station, or between the first station and a user at the second station, the shared parameter being encrypted using said session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station (authentication of parties of communication to each other and verification of session key based on a shared secret was well-known in the art at the time of invention. Kelly col. 7 lines 5-50 provides a matching example. Specifically, after the session key is established, in item (d) of the authentication protocol, a password (shared secret) is encrypted using the session key and sent to the host. The host verifies the password, and authenticates the other party),

- In another exchange in the plurality of exchanges, sending, after verifying in said first station receipt of the session key by the second station, at least one message carrying an encrypted version of one of the intermediate data keys from said set of intermediate data keys to be accepted as the symmetric encryption key for use by the first and second stations during the communication session (Perlman col. 5 line 5 to col. 6 line 57, where it teaches exchanging ephemeral keys to be used as encryption keys for limited periods of time (session) between the two parties of communication).

Perlman and Kelly are analogous art as they are both directed to key distribution and user authentication in security systems based on cryptographic processes.

At the time of invention, it would have been obvious to the person skilled in art to combine the method of secured key exchange as taught by Kelly with the method of ephemeral key distribution as taught by Perlman. Kelly teaches a method to securely deliver keys from one party to another. Perlman teaches use of multiple ephemeral keys to secure the communication session, which requires transmission of ephemeral keys from one party to the other. Therefore, the one skilled in art would be motivated to use the method of Kelly to deliver the ephemeral keys of Perlman from one party to the other.

7.2. In reference to claim 2:

Art Unit: 2132

Perlman (Column 2, lines 45 - 67) discloses the method of claim 1, including assigning said session random key to all communication sessions initiated with the first session, during said session random key initiation interval, where the session random keys are the ephemeral keys used for communications between the first and second parties.

Note that the purpose of ephemeral keys is to be used as the encryption key to encrypt messages exchanges between parties in the lifetime of the ephemeral key, and replacing the current ephemeral key with another key when the lifetime of the current key is expired.

7.3. In reference to claim 3:

Perlman discloses the method of claim 2, including assigning said session random key to all communication sessions initiated with the first station during said session random key initiation interval, and associating a different set of ephemeral intermediate data random keys with each communication session, where the first party announces a set of ephemeral key pairs (Column 5, lines 55-67) and each time the second party desires to launch a communication session with the first party, a key is selected from the list (and therefore is unique), and the first party passes the key to the second party (Column 6, lines 1-20).

7.4. In reference to claim 4:

Perlman discloses the method of claim 1, including

Art Unit: 2132

- Providing a buffer at the first station; (Perlman Column 6, lines 35-57)
- Storing an ephemeral set of session random key in the buffer for respective session key lifetimes; (Column 5, lines 55- 67 & Column 6, lines 35-57. Note that the session keys are ephemeral keys and are stored only during their lifetime)
- Associating respective session key initiation intervals with said session keys stored in said buffer. (Column 5, lines 55 - Column 6, lines 20)
- Using session keys from the set of session keys from said buffer as session keys in response to requests received by said first station during said respective associated session key initiation intervals. (Column 5, lines 55 - Column 6, lines 20. Perlman's teaching of ephemeral keys is for the purpose substituting a key with another after the lifetime of a key is expired. Therefore, the session keys are substituted with a fresh key after expiration of their lifetime)
- Removing session keys from said buffer upon expiry of the respective session key lifetimes (Column 6, lines 35- 57).

7.5. In reference to claim 6:

Perlman discloses the method of claim 4, wherein the session key lifetimes have respective lengths longer or equal to time required for the plurality of exchanges used to



Art Unit: 2132

distribute the symmetric encryption key for use in communication session can be completed in expected circumstances (Column 6, lines 35-67. The lifetime of Perlman's ephemeral keys is arbitrarily set to match the application. Setting the lifetime such that it is usable after the set up period is completed is a logical and obvious choice).

7.6. In reference to claim 7:

Perlman discloses the method of claim 4, wherein the session key lifetimes have respective lengths which are multiple  $M$  times a time required for the plurality of exchanges used to distribute the symmetric encryption key for use in communication session can be completed in expected circumstances, where  $M$  is less than or equal to 10. (Column 6, lines 35-67. The lifetime of Perlman's ephemeral keys is arbitrarily set to match the application. Setting the lifetime such that it is usable after any multiple of time it takes to complete the set up period is a logical and obvious choice).

7.7. Requirements of claims 8-11, 13-18, 20 and 21 are substantially the same as claims 1-4, 5-7 discussed above.

7.8. In reference to claim 22:

Perlman discloses the method of claim 1, wherein the encrypted version of one of said set of intermediate data keys to be accepted as the symmetric encryption key is

encrypted using a shared secret credential (encrypting a key using a shared is a widely known technique and an obvious choice to protect the key during key exchange).

7.9. In reference to claim 23:

Perlman discloses the method of claim 1. The additional requirements of claim 23 are an iterative method, which involves application of a set of operations in each iteration, each of those operations identical to one of the operations discussed above. Namely, during the first to the  $(n-1)$ th iteration, the system repeats sending a new key, encrypted from one station to the other. The new key is encrypted with a key known to both parties (the previous session key). The receiving side decrypts the encrypted new key and uses it as the new session key. This whole process is discussed in claim 1. In the  $n$ th and  $(n+1)$ th iteration, the same process continues, with the exception that in the  $n$ th iteration the shared secret is used to encrypt the new key, and in the  $(n+1)$ th iteration a second shared secret is use for the same. This technique is also discussed above. The  $n$ th and  $(n+1)$ th iterations also includes creating a hash of the session key, which is also a well-known technique in the art. Therefore, all steps of the iterative method are discussed, and shown as prior art in the above. Also, using an iterative technique to improve the security of the cryptographic protocol is well known in the art. Reference is made to the DES protocol, which basically deploys a plurality of stages that scrambles the input data iteratively, and each iterative stage uses a different parameter (a key) to perform a different operation. The key in each stage is extracted from the previous stage. As another example, reference is made to "Applied Cryptography" by B. Schneier, page 53

Art Unit: 2132

(a copy is attached to this Office Action). Section titled SKEY, clearly teaches the concept of repeated application of a cryptographic technique to improve the security of the protocol. Therefore, given enough resources and time, it would have been obvious to use an iterative method, which includes a known process at each iterative stage to improve the security of the protocol.

7.10. In reference to claim 24:

Perlman discloses the method of claim 1. The additional requirements of claim 24 are substantially the same as claim 23, with the exception that in the nth iteration, the nth key is encrypted using the first shared secret and the intermediate data key (n-1), which is also a known technique.

7.11. Requirements of claims 25-30 are substantially the same as claims 1-4, 5-7, and 22-24 discussed above.

### ***Conclusion***

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2132

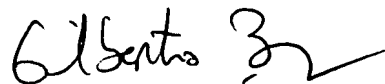
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

**Farid Homayounmehr**



GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100